PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 94/08409
H04L 9/08	A1	(43) International Publication Date:	14 April 1994 (14.04.94)

(21) International Application Number: PCT/GB93/02075

(22) International Filing Date: 6 October 1993 (06.10.93)

(30) Priority data:
92309126.8 7 October 1992 (07.10.92) EP
(34) Countries for which the regional or international application was filed: AT et al.

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PLC [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

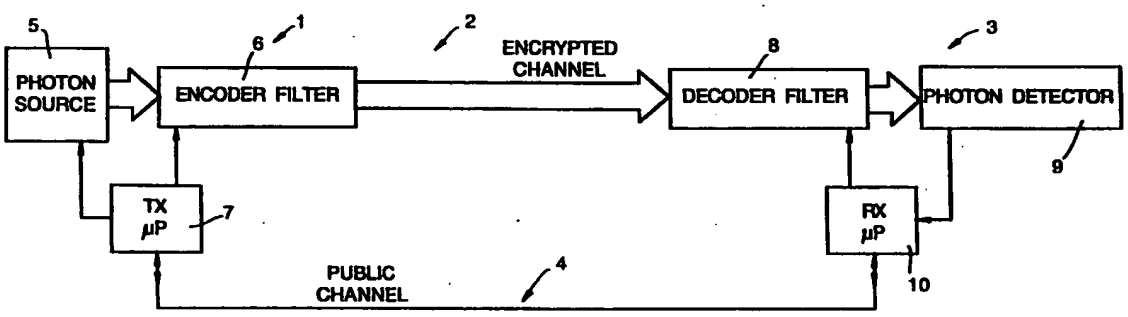
(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : PHOENIX, Simon, James, Daniel [GB/GB]; 31 The Street, Bawdsey, Woodbridge, Suffolk IP12 3AH (GB). BARNETT, Stephen, Mark [GB/GB]; 4 Bower Street, Hillhead, Glasgow G12 8PT (GB).

(74) Agent: GILL JENNINGS & EVERY; Broadgate House, 7 Eldon Street, London EC2M 7LH (GB).

(81) Designated States: AU, CA, JP, KR, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: QUANTUM CRYPTOGRAPHY USING DISCARDED DATA



(57) Abstract

A communication system uses single-channel quantum cryptography for the secure transmission of a key. A transmitter randomly selects one of a number of encryption alphabets corresponding to different non-commutating quantum mechanical operators. The transmitter and receiver then subsequently communicate to establish which of the transmitted signals were encoded and decoded using common operators. The signals which were transmitted and received using different operators, the discarded data, are analysed and the expected and measured statistics compared to determine whether an eavesdropper has intercepted the transmission. In a preferred example, the transmitter selects from three or more different encoding alphabets comprising at least two mutually orthogonal alphabets and one other intermediate alphabet. In this case, separate statistical tests may be applied to the discarded data encoded with the orthogonal alphabets and to the discarded data encoded with the intermediate alphabet.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NE	Niger
BE	Belgium	GN	Guinea	NL	Netherlands
BF	Burkina Faso	GR	Greece	NO	Norway
BG	Bulgaria	HU	Hungary	NZ	New Zealand
BJ	Benin	IE	Ireland	PL	Poland
BR	Brazil	IT	Italy	PT	Portugal
BY	Belarus	JP	Japan	RO	Romania
CA	Canada	KP	Democratic People's Republic of Korea	RU	Russian Federation
CF	Central African Republic			SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovak Republic
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	UA	Ukraine
DE	Germany	MG	Madagascar	US	United States of America
DK	Denmark	ML	Mali	UZ	Uzbekistan
ES	Spain	MN	Mongolia	VN	Viet Nam
FI	Finland				

QUANTUM CRYPTOGRAPHY USING DISCARDED DATA

BACKGROUND TO THE INVENTION

The present invention relates to a system for communicating data using cryptographic techniques. In particular, it relates to a development of the technique known as quantum cryptography.

There are many situations in which communication between two or more parties needs to be made secure so that any unauthorised party cannot gain access to the transmitted data. Since in general it is not possible to ensure that the physical channel over which the communication takes place is inaccessible to unauthorised parties or "eavesdroppers", protection of sensitive communications is normally achieved by the use of cryptographic techniques. This entails the encipherment of *plaintext* (the data) and the subsequent decipherment of the *ciphertext* (the encrypted data) back into plaintext. The encipherment and decipherment in general are determined by some specified algorithm using a key. The algorithm is assumed to be freely available to all users of the channel whether authorised or otherwise. Accordingly the security of the transmission depends upon the key remaining secret and being unknown to any eavesdropper. In the type of system the present invention is concerned with, the key is shared in common between authorised users of the channel. The operation of the system therefore depends upon being able to transmit securely a secret key to the legitimate users of the channel.

It has previously been proposed to use a technique, developed at IBM and elsewhere, known as quantum cryptography, for the distribution of the key in such a way that the security of the key can be guaranteed. This technique which might more appropriately be termed "quantum key-distribution" relies on the use of a protocol designed to take account of the non-commutativity of quantum mechanical operators. This property makes it possible to detect the presence of an eavesdropper through a change in

the statistics of the data reaching the receiver. The theory underlying this is discussed in further detail below.

There are currently two distinct methods of achieving key security using quantum cryptography. One scheme exploits the properties of correlated quantum channels. The other employs just a single quantum channel. It is to this latter kind of channel that the present invention relates.

In general then a method of operating a communication system using single-channel quantum cryptography includes the steps of:

(a) randomly selecting at the transmitter one of a plurality of coding alphabets corresponding to different, non-commutating quantum mechanical operators and encoding a signal for transmission to the receiver using the selected operator;

(b) randomly selecting at the receiver one of the different quantum mechanical operators and using that operator in detecting the signal transmitted in step (a);

(c) repeating steps (a) and (b) for each of a multiplicity of subsequent signals;

(d) communicating between the transmitter and the receiver to determine for which of the transmitted signals common operators were selected by the transmitter and receiver;

(e) comparing the signals transmitted and received in steps (a) and (b) to detect any discrepancy resulting from the presence of an eavesdropper; and,

(f) in the event that in step (e) no eavesdropper is detected using at least some of the data transmitted in steps (a) and (b) as a key for encryption/decryption of subsequent transmissions.

SUMMARY OF THE INVENTION

According to the present invention, a method of operating a communication system using single-channel quantum cryptography is characterised by analysing data

determined to have been transmitted and detected using different operators at the transmitter and receiver and comparing the expected and measured relationship between the data transmitted and received to detect whether an eavesdropper is present.

As described in further detail below, quantum cryptography involves communication between the transmitter and receiver to determine which transmitted and detected bits were transmitted and received using the same quantum operators. For example, in the Bennett-Brassard quantum key-distribution technique described in further detail below, the transmitter randomly selects between alphabets formed from different linear polarization states or different rotational polarization states. The transmitter and receiver then subsequently communicate to determine which signals were both encoded and decoded as different linear states and which were both encoded and decoded as different circular polarization states. Hitherto solely these signals have been used for the transmission of useful data and also for the detection of any eavesdropper. Those signals encoded and decoded using different operators, for example a signal encoded in different linear polarization states but detected in terms of different rotational polarization states, have conventionally been "rejected", and such data are termed herein "rejected data". The present inventor has realised that improved security can be obtained by carrying out tests on the "rejected" signals, so as to increase the chance of detecting any eavesdropper while at the same time potentially leaving the un-rejected signals free for the carrying of useful data.

The method may include the steps of both comparing the statistics of the transmitted and received rejected data to determine whether any eavesdropper has detected the communicated signal using a different quantum alphabet to those used by the transmitter and receiver; and also

subsequently testing at least a sample of the other data to determine whether any eavesdropper has detected the

communicated signal using a coding alphabet used by the transmitter and receiver.

Preferably however testing to detect an eavesdropper is carried out using rejected data only. In this case preferably the transmitter encodes data using a selected one of three or more different coding alphabets, the three or more coding alphabets having symbols which are eigenstates of mutually non-commuting operators, and the detector detecting signals using at least two of the alphabets. Preferably the transmitter encodes the signals using one of spin-z, spin-$\pi/3$ and spin-$2\pi/3$ alphabets and the receiver decodes the signal using at least two of the three transmitted alphabets. In this case separate tests are preferably carried out on discarded data encoded with the z, $\pi/3$ alphabets, the z, $2\pi/3$ alphabets and $\pi/3$, $2\pi/3$ alphabets at the transmitter and receiver. It should be noted that, in accordance with the general theorem of K.J. Blow and S.J.D. Phoenix, J. Mod. Opt., 40 33 (1993), the receiver need only measure in two of the transmitted alphabets to achieve protection against eavesdropping. However, at least one of the users Alice and Bob need to use at least 3 alphabets for a rejected-data protocol to work.

According to a second aspect of the invention there is provided a communication system comprising a single photon source and a single photon detector arranged to be connected to a communications channel, means for encoding a single photon signal from the single photon source using non-commuting quantum mechanical operators, means for detecting using non-commuting quantum mechanical operators a single photon signal received over the communications channel, and processing means for comparing the states of single photon signals as encoded and detected, thereby detecting the presence of any eavesdropper,

characterised in that the processing means include means for analysing data determined to have been encoded and decoded using different operators and comparing the

expected and measured relationship between the data encoded and detected to detect any eavesdropper.

BRIEF DESCRIPTION OF THE DRAWINGS

An example in accordance with the present invention and the theoretical background to the present invention will now be described in further detail with reference to the accompanying drawings, in which:

Figure 1 is a diagram illustrating the mapping of an operator onto three orthogonal spin directions;

Figure 2 is a diagram illustrating the transmission paths between users of the communication system and an eavesdropper;

Figure 3 is a diagram illustrating different probability pathways for data encoded and decoded using a common operator in the presence of an eavesdropper;

Figure 4 is a diagram showing probability pathways for transmissions in a system in accordance with the present invention with an eavesdropper re-transmitting in an intermediate alphabet;

Figure 5 is a block diagram showing the layout of an example of a communication system in accordance with this invention;

Figure 6 is an example of a single-photon source;

Figure 7 shows a network used in implementing the invention; and

Figures 8a and 8b are examples of polarisation modulators in a transmitter and receiver respectively for use in the network of Figure 7.

Figure 5 shows a system suitable for implementing the quantum cryptography technique of the present invention. A transmitter 1 transmits encrypted data over a channel 2 to a receiver 3. The receiver and transmitter are also in communication via a second channel 4. In the present example the encrypted channel is carried optically on a passive optical fibre network. It will be understood however that the present invention is by no means limited in applicability to optical networks, but may be used with

other communication channels such as, for example, radio links.

The transmitter 1 includes a single photon source 5, the output of which is sent to an encoder filter 6. The encoder filter 6 uses an electro-optic polarisation modulator to alter the states of polarization of single photons. In the present example, the modulator is a Mach-Zehnder interferometer with a phase modulator in one arm, switching at, say, 10 MHz. The photon source 5 and encoder filter 6 are controlled by a first microprocessor 7.

Figure 6 shows in further detail the photon source 5 used in this example. A laser 51 which may be, e.g. a Ti:Sapphire at 750 nm, is used to pump a nonlinear crystal 52, e.g. KDP. The parametric downconversion effected by the crystal produces correlated twin beams of photons at 1.5 μm. The photons in one beam are detected by a photodetector 53 and this triggers a gate 54 which opens a shutter to let through a single photon.

The receiver 3 employs a complementary architecture with the incoming optical signal being received via a decoder filter 8 at a photon detector 9. The output of the photon detector 9 is fed to a second microprocessor 10 which also controls the decoder filter 8. As in the transmitter, the decoder filter may be formed from an electro-optic polarisation modulator. Data is also transmitted between the microprocessors in the transmitter and receiver via the second channel 4.

As will be described in further detail below, the encoder and decoder filters are controlled by their respective microprocessors to encode or decode photons in different linear polarization states or different rotational polarization states. Each microprocessor contains a record of which states have been encoded or measured for each bit which is transmitted. This information is exchanged via the public channel 4. Using this information the statistics of the received data are calculated and compared with the expected data. On the

basis of this comparison it is determined whether there is any eavesdropper intercepting the data communicated on the encrypted channel 2. Although Figure 5 shows only a single transmitter/receiver pair, in practice the present invention may be employed in systems using multiple-access networks, for example employing ring, star or tree topologies, as described and claimed in the present applicant's co-pending European Patent application no. 93307120.1, incorporated herein by reference.

Figure 7 shows a specific example of a broadcast network containing two receivers and a transmitter. The transmitter 1 consists of a gain-switched semiconductor laser 79, which may be a DFB or Fabry-Perot device, an attenuator or intensity modulator 77, and a polarisation modulator 78 and control electronics 70. The single-photon detectors in the receivers may be avalanche photodiodes (APDs) biased beyond breakdown and operating in the Geiger mode with passive quenching, as discussed in P. D. Townsend, J. G. Rarity and P. R. Tapster, Electronics Letters, 29, 634 (1993). Silicon APDs such as the SPCM-100-PQ (GE Canada Electro Optics) can be used in the 400-1060 nm wavelength range, while Germanium or InGaAs devices such as the NDL5102P or NDL5500P (NEC) can be used in 1000-1550 nm range.

Although APD's are the preferred form of detector, the present invention is not limited to the use of APD's. Other detectors having appropriate sensitivity and discrimination at the single-photon level may be used. For example, the detector may use a photomultiplier tube. Each receiver 3 includes a microprocessor control unit 72, which receives the output of the APD via a discriminator/amplifier circuit 73. The control unit 72 also controls an electronic filter 74 and local oscillator 75, as well as the APD bias supply 76. The electronic filter 74 isolates the first harmonic of the frequency spectrum of the signal output by the APD in response to synchronising pulses received via the network. This

generates a sinusoidal signal at the pulse frequency which locks the local oscillator 75. The output of the local oscillator 75 is received at the control unit 72 to provide a timing reference during quantum transmissions.

The use of multi-photon signals on the transmission medium to calibrate the system prior to or during quantum transmission is described in further detail in our co-pending British patent application no. 9226995.0, filed 24/12/92 entitled Communications System and incorporated herein by reference. This makes it possible to compensate, e.g. for changes in fibre polarisation resulting from environmental effects.

The key distribution process is initiated by the transmitter sending a stream of timing pulses into the network. The attenuator in the transmitter is not engaged at this point, so the pulses contain many photons and are received by both terminals. The receivers set the reverse bias on their detectors to be well-below breakdown so that the internal gain is low. In this mode the APDs can detect the multi-photon timing pulses without suffering from saturation. Each APD output signal will contain a frequency component at the fundamental repetition rate of the pulsed source, and this is used to lock the local oscillator in the receiver as described above.

After the synchronisation procedure the attenuator in the transmitter is engaged so that the output pulses contain on the order of 0.1 photons on average. In addition, the APDs in the receivers are biased beyond breakdown so that internal gain is high enough to achieve detection sensitivity at the single-photon level. Steps (a) to (c) of the quantum key distribution protocol are then carried out. In the current example, the system uses an encoding scheme in which polarisation states are used to establish the sequences of key bits.

Figure 7 shows the details of the polarisation modulators in this example. The transmitter modulator is based on a 6-into-1 optical switch that is switched

randomly so that for each pulse one of the six possible polarisation states is coupled into the network. The optical switch could be based on one or more electro-optic devices (e.g. United Technology lithium niobate Y-switch "YBBM") and the 6x1 coupler could be a fused fibre device (e.g. Sifam Fibre Optics P4S13C). The polarisation modulators in the receivers are similar in design. However, here the different polarisation channels contain fibre delays of differing lengths. This allows a single APD to be used at the output, with polarisation state identification performed by means of the time (within the laser period) at which the photo-count occurs. A similar detection scheme to this is described in A. Muller, J. Breguet and N. Gisin, Europhysics Letters 1993 (submitted).

In the steps (a) to (c), a sufficient number of single photon pulses need to be transmitted for each receiver to establish the required number of key bits. The topology of optical fibre path from the control node to the terminals depends on the network architecture. For example, the path may split via a single 1-into-n coupler or some other combination of 1-into-m couplers, where n is the number of terminals on the network and $m < n$. The probability that any given photon arrives at a terminal from the central node is given by the transmission coefficient for that specific path, $t=\exp -(\alpha l + \beta)$, where α is the fibre loss coefficient per unit length, l is the path length and β is the net coupling ratio for the path. The quantum mechanical properties of single photons ensure that a given photon will either be detected at one, and only one, of the terminals or will be lost from the system ($\alpha > 0$), and that this process occurs in a totally random and unpredictable way. Consequently, each terminal has no way of predicting whether or not a photon will arrive during a given clock period. Instead, all terminals make measurements as described in step (b) at the clock rate, and for each successful detection of a photon record the alphabet used

for he measurement, the actual result of the measurement and the time-slot in which the photon arrived.

After completing the quantum transmission, the central node sequentially polls each of the terminals on the network and carries out steps (d) to (f) of the protocol. In this process the individual photons and their sent and received states are identified by means of the time-slot in which they were detected and transmitted. The statistics of the rejected data for the transmitter and each respective receiver are determined, and compared with an appropriate threshold for detection of any eavesdropper. At the end of this process the central node is in possession of n secret keys, each one shared with a specific termninal on the network. However, each terminal has no knowledge of any other key apart from its own. These keys can now be used to securely encrypt data transmissions between each terminal and the central node. Consequently, any encrypted data that is broadcast from the transmitter can only be read by the terminal for which it is intended. In addition, the terminals can communicate securely with each other via the central node which acts as a secure interpreter. The public discussion stages (steps (d) to (f)) described above may be carried out over the same network or over a separate and independent communication channel.

Practical quantum channels, suffer from unavoidable background error rates due to detector dark counts, and environmentally-induced fluctuations in the polarisation (or phase) state in the fibre etc. In this case the public discussion phase may contain an additional stage of error correction and so-called "privacy amplification". This both ensures that the transmitter and receiver end up with identical keys and that any key information leaked to an eavesdropper is an arbitrarily small fraction of one bit. This procedure is outlined in C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: "Experimental Quantum Cryptography", J. Cryptology, 5, 3 (1992).

Although in the example of Figure 7 only two receivers are shown, in practice networks employing greater numbers or receivers will often be used. The number chosen will vary according to the field of use. For a local installation on a single site, the network might comprise only 10 receivers or terminals. By contrast, for a public network several 10's or even a 100 or more receivers might be connected to the network and would receive quantum keys distributed from a single server.

The present invention may also be implemented in networks including a looped-back path from the receiver to the transmitter. The transmitter may then, as part of the protocol, carry out comparisons on the states of photons as output from the transmitter and received back at the transmitter on the looped-back path. The receiver may include a modulator for encoding a received photon before returning it on the looped-back path to the transmitter. Systems of this sort are disclosed and claimed in our co-pending European Patent application No. 93307121.9, incorporated herein by reference.

The discussion below sets out in further detail the theory underlying the method of the present invention and relates it to prior art quantum cryptography techniques.

QUANTUM CRYPTOGRAPHY

Quantum cryptography is a technique, for the distribution of key information in such a way that the security of this information can be guaranteed. The technique relies on two crucial elements: the non-commutativity of quantum mechanical operators (that is, $\hat{A}\hat{B} \neq \hat{B}\hat{A}$) and a protocol designed to take advantage of this physical phenomenon. We describe below the simple system considered originally by Bennett et al.. [1] This system relies on two alphabets with just two symbols each but the concepts can be generalized to include alphabets of arbitrary size. [2]

The Bennett-Brassard (BB, for convenience) quantum key-distribution technique relies on the properties of

single photons. One bit of information can be encoded in the linear polarisation (a logical "1" for vertical polarisation and a logical "0" for horizontal polarisation). Similarly one bit of information can be encoded in the circular polarisation (a logical "1" for right circular polarisation and a logical "0" for left circularly polarised photons). It is well-known that any two-state quantum mechanical system can be described by a spin algebra so that the polarisation variables can be mapped directly onto spin variables. The polarisation states of the photon can, mathematically, be treated as spin variables. A spin (polarisation) operator has two eigenstates "up" and "down". Thus with reference to Figure 1, we can say that the spin operator in the direction characterised by θ,ϕ has two eigenstates which we label $|+>_{\theta,\phi}$ for the "up" state and $|->_{\theta,\phi}$ for the "down" state. The spin analogues of the linear and circular polarisation operators are the spin in the z-direction and spin in the x-direction. The advantage of using the spin variables is that, for may purposes, the angle θ can be used to describe an intermediate spin and one can envision the arrow in Figure 1 moving on the surface of a sphere. A similar picture for polarisation, whilst possible, is not as transparent.

The spin operators in the x and z directions do not commute. This is purely a quantum mechanical phenomenon and leads to the result that the eigenstates of the spin-z operator can be expressed as linear superpositions of the spin-x operator. (This is a standard quantum mechanical result described in all good textbooks of quantum mechanics). If a photon is transmitted in the $|+>_z$ state so that a logical "1" is sent and the receiver chooses to measure the spin-x variable the probability that the receiver reads a logical "1" also is just the modulus of the overlap squared, $|_x<+|+>_z|^2$. This simple result has far-reaching consequences and results in the possibility of secure key distribution. Implicit in this result is the

possibility that by measuring the spin-x variable the receiver can read a logical "0" when a logical "1" was transmitted. In this discussion we shall adopt the terminology [1] that "Alice" is the transmitter and "Bob" is the receiver. Let us now suppose that Bob, the receiver, has in fact tried to measure the spin-x operator when Alice has transmitted the bit of information encoded on the eigenstates of the spin-z operator and has read a logical "0", that is, he has measured the spin-x component and found it to be in the spin "down" eigenstate. We shall assume that Alice was in fact trying to convey a logical "1" to Bob, in which case she actually sent the state $|+>_z$. If Bob does not communicate in some other way with Alice he has no way of knowing that his result is incorrect. As far as Bob can determine Alice transmitted the state $|-\rangle_x$. Bob has, therefore, irretrievably corrupted the data encoded by Alice. The uncertainty principle prevents Bob from trying to measure both spin directions at once, or at least ensures that any results of so doing will be meaningless. The next point to notice is that in order to read the data Bob must measure the spin (polarisation) of a single photon and therefore projects the photon state onto an eigenstate of his measured spin. From a physical point of view there is no difference between the action of an eavesdropper and Bob. Any eavesdropper (whom we shall call "Eve") must perform spin (polarisation) measurements in order to access the information encoded in the photon state. Eve will also collapse the wavefunction onto an eigenstate of her chosen spin operators. Eve must then retransmit the photon onto Bob. The crucial point is this: if Eve has measured a different spin to that used by Alice in transmission then Eve will transmit an eigenstate of her operator (different to that of Alice) on to Bob. Bob has then only a probability less than one of reading the correct logical symbol even if he measures the same spin operator that Alice used. Now if Alice and Bob have used the same spin

operator they would expect to agree on their message, that is, if Alice transmits a "1" then Bob will expect to read a "1" with unit probability. However, if Eve has attempted to intervene then she may have tried to measure in the incorrect spin direction and the subsequent wavefunction collapse onto an eigenstate of this operator will result in Alice and Bob having the same logical symbol with a probability of less than unity. In effect by measuring in the wrong direction Eve "scrambles" the data in the correct direction. It is the possibility, in quantum mechanics, of using non-commuting operators to transmit information which leads to this unavoidable disturbance by the eavesdropper.

We now describe the protocol, developed by Bennett et al.,[1] which makes use of this quantum mechanical non-commutativity of the operators associated with physical observables.

1. Alice randomly selects one of the four states $|\pm>_z$ and $|\pm>_x$ to transmit to Bob. She makes a record of which state she transmits.

2. Bob randomly selects which spin (polarisation) direction to measure and makes a record of the result.

3. Alice and Bob now communicate over a public channel. They select a randomly-chosen, but identical, subset of their transmitted and received data and reject all those for which different spin directions were chosen. In the absence of any eavesdropper Alice and Bob should now have a string of identical bits.

4. Alice and Bob now compare their data for any deviation from this perfect agreement. If any discrepancy is discovered Alice and Bob can now conclude that there has been an attempt at eavesdropping. If their data is in agreement the bits used for the eavesdropping test are discarded and Alice and Bob now consider their remaining data. The bits which were transmitted and received in different directions are discarded as before. The remaining data, free from any interception by an eavesdropper, consists of those bits for which Alice and

Bob used the same spin (polarisation) direction and Alice's data should be identical to Bob's. This data, which has not been communicated publicly and has been transmitted over a channel which is known to be eavesdropper-free by virtue of Alice's and Bob's previous comparison, is now shared secret information between Alice and Bob. This secrecy is guaranteed by virtue of the laws of quantum mechanics and the protocol which exploits this. The key cannot even in principle be deduced, except by blind guesswork, and cannot be calculated no matter how powerful the computational facilities available.

The above is a description of the protocol developed principally at IBM and it exploits the properties of a single quantum channel. Another technique has been developed [3] [4] which exploits the properties of correlated quantum channels and the statistical test for the eavesdropper is based on the violation of the Bell inequalities. This system has been shown[5] to give equivalent security to that of the BB scheme. However, the protocol required to exploit these correlated channels is different and does not sacrifice any of the potentially useful key data in the test for the eavesdropper. The present invention relates to single quantum channels and describes a method whereby eavesdropping can be detected on these channels without having to sacrifice any key data. The prior art protocol for single channels (the BB protocol) rejects approximately half of the data (for alphabets of higher dimensionality this fraction is greater). The new protocol, described below, can be applied to single quantum channels of dimensionality $N \geq 2$ and is a technique for using the "rejected" data to yield information about an eavesdropper.

The present invention is based on the realisation that the rejected data can give useful information about the eavesdropper. This realisation has been facilitated by our development of a formalism which treats the quantum states as symbols of an alphabet. The alphabet is taken to be a

set of eigenstates of a particular operator. In terms of the photon polarisation variables the linear polarisation alphabet consists of two symbols | *horizontal* > and | *vertical* >. In terms of the spin variables the spin-z operator generates an alphabet of two symbols $| \pm >_z$. The channel transition probabilities can then be determined from the a priori probabilities and the overlap integrals between the states of the transmitter and receiver alphabets. The normalized difference between the information flow rates on the interrupted and uninterrupted routes yields a parameter ξ which varies between -1 and +1. This parameter determines by how much the eavesdropper disturbs the channel. The BB protocol is designed to exploit the region where ξ is negative so that the presence of the eavesdropper reduces the flow of information between Alice and Bob. However, our analysis shows that an eavesdropper can also increase the flow of information, that is $\xi > 0$, and it is this increase of information which can betray the presence of the eavesdropper. In the extreme case, which we will describe later, Alice and Bob can choose alphabets such that, in the absence of an eavesdropper, there is no flow of information between them. Any attempt to eavesdrop this channel will result in the creation of an information flow between Alice and Bob which can be detected. We describe below the additional protocol necessary to exploit the positive ξ region. Essentially the rejected data can be used because the eavesdropper will introduce a deviation from the expected statistics of this data. This deviation is an unavoidable consequence of the attempt to eavesdrop. Once again the laws of physics conspire to foil the hapless intruder.

The Bennett-Brassard Protocol

Much of the following discussion will relate to Figure 2 in which we schematically depict Alice and Bob connected by two communication paths. Pathway 3 is a direct link and is not eavesdropped by Eve. Pathway 12, via Eve, is the

path along which Alice and Bob will attempt to communicate using their quantum alphabets. Alice and Bob will use the alphabets generated by the spin-x and spin-z operators. Eve will be free to measure in any particular alphabet between these spins characterized by the angle θ. (This angle is included because we shall shortly be discussing Eve's optimum strategy and this involves a measurement of the spin at an angle $\pi/4$, with respect to the spin-z operator[1]). The results of Alice transmitting in any of her possible states are summarized in the table below (Figure 4). Let us follow through some of the possible transmissions and results by way of example. Suppose that Alice's random choice has resulted in a transmission of the state $|+\rangle_z$ which is, of course equivalent to a logical "1". Eve attempts to determine this bit by measurement of spin in the x-direction. The rules of quantum mechanics tell us that in Eve's alphabet the transmitted state is expanded as follows

$$|+\rangle_z = \frac{1}{\sqrt{2}}(|+\rangle_x + |-\rangle_x) \qquad (1)$$

Again following the rules of quantum mechanics if Eve measures the x-direction spin (polarisation) then she will find the photon in the state $|+\rangle_x$ with probability of 1/2 and in the state $|-\rangle_x$ also with a probability of 1/2. Eve has no way of knowing, at this stage, that she has measured the incorrect alphabet. Let us suppose that she reads the symbol "1" and retransmits this to Bob as the state $|+\rangle_x$. We shall assume that Bob has randomly chosen to measure the spin-z variable. He will obtain the result "1" with probability of 1/2, thereby believing that the state $|+\rangle_z$ has been transmitted. However, he will obtain the result $|-\rangle_z$ and therefore read the symbol "0" with probability of 1/2. If Alice and Bob now communicate and discover that they have used the same alphabet they would expect that they have the same symbol, that is "1".

However, Eve's intervention means that there is a finite probability, per bit, that Alice and Bob will disagree even when they choose the same alphabets. The probability pathway if Alice sends "1" in the z-direction, and Alice and Bob have rejected the data for which they used different alphabets, is shown in Figure 3. The probability that Alice and Bob agree, and therefore also the probability that Eve escapes detection per bit, is just 3/4. If Eve had not been trying to eavesdrop then Alice and Bob would agree with unit probability. A similar analysis for the other possible states that Alice could transmit yields the same error probability for Alice and Bob. Therefore, if Eve is attempting to eavesdrop using the alphabets employed by Alice and Bob she has a 3/4 chance, per bit, of escaping detection. If Alice and Bob compare N bits of data Eve's chances of escaping detection are just $(3/4)^N$, which becomes extremely small as N increases (a probability of escaping detection of approximately 0.06 if only 10 bits of data are compared - but in practice many bits would be compared and this probability of escaping detection becomes approximately 3.2×10^{-13}, that is, about 3 chances in 10 trillion of escaping detection, if 100 bits are compared).

The other important parameter to determine is exactly how much of the data, on average, that Eve is able to determine correctly. Thus in the previous example Eve will read the symbol "1" 3/4 of the time and this follows through to the other possible transmissions so that Eve's chance of reading the correct bit, per bit, is 3/4. Thus, in the almost inconceivable event that Eve escapes detection, she will still only have approximately 75% of the key correct. Eve can maximise her knowledge of the correct key by measuring in the Breidbart basis[1]. This alphabet is generated by the spin in a direction oriented by an angle of $\pi/4$ with respect to the spin-z operator. Referring to the tables we find that Eve's best strategy is to measure this alphabet and retransmit symbols in this

alphabet so that after calculation of the relevant probability pathways as before it is found that Eve's probability of escaping detection is still just 3/4 per bit. However, her chances of obtaining the correct bit are now increased to

$$\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \approx 0.85$$

that is Eve can determine, at least in a statistical sense, approximately 85% of the key. Eve's optimum strategy, with this protocol, is to measure the alphabet associated with this Breidbart bases. [1] [5] The present invention, using the protocol described below is a development of the BB protocol which reduces the effectiveness of an attack in the Breidbart basis by examination of the rejected data rather than examination of a subset of useful data.

Rejected Data Protocol [6]

We shall describe how the new protocol of this embodiment of the present invention can be implemented to give extra security within the $N = 2$ alphabet that we have already discussed above. It is important to note that although we shall employ a specific example the method is, in its broad essentials, valid for any size of alphabet. Firstly let us consider Alice's and Bob's results in the absence of Eve, the eavesdropper. This is achieved in the table of probabilities by setting $\theta = 0$ for the spin-z transmissions of Alice and $\theta = \pi/2$ for the spin-x transmissions. We shall now consider those results for which Alice and Bob used a different alphabet. Suppose Alice sends the state $|+>_z$, that is, a logical "1". Bob, by assumption is measuring in the spin-x direction (that is, in the direction different to that of Eve) and he will obtain the result "1" half of the time, on average, and the result "0" half of the time, on average, only half of their data in agreement.

Suppose now that Eve attempts to eavesdrop in the spin-z or spin-x directions. We shall assume that Alice sends the state $| + >_z$ as before. If Eve measures the spin-z direction she will obtain the result "1" with a probability of unity and transmit the state $| + >_z$ on to Bob. Remembering that we are only interested, at present, in Alice and Bob using different alphabets, then by assumption Bob measures the spin-x operator. He will obtain the result "1 with probability of 1/2 as before. Suppose now that Eve eavesdrops in the spin-x direction, that is, she chooses the angle $\theta = \pi/2$ in the probability table. Eve then transmits on to Bob the state $| + >_x$ or $| - >_x$ with equal likelihood, which Bob reads without error as his measurement is aligned in this direction. Alice and Bob still disagree, on average, 1/2 of the time. Thus if Eve measures spin-x or spin-z, that is, the alphabets Alice and Bob are using, then the rejected data gives no information about Eve.

Let us now suppose, however, that Eve decides to try an attack on the channel by using some basis aligned at an angle θ. Alice transmits $| + >_z$ and Bob measures spin-x as before. Reading the probabilities off the table we find that Eve reads "1" with probability of $\cos^2\theta/2$ and, therefore, transmits the state $| + >_\theta$ on to Bob who then reads "1" with probability 1/2 $| \cos\theta/2 + \sin\theta/2 |^2$ and "0" with probability 1/2 $| \cos\theta/2 - \sin\theta/2 |^2$. Similarly, if Eve reads "0" (probability $\sin^2 \theta/2$) and therefore transmits the state $| - >_\theta$ on to Bob, then Bob reads "1" with probability 1/2 $| \cos\theta/2 - \sin\theta/2 |^2$ and "0" with probability 1/2 $| \cos\theta/2 + \sin\theta/2 |^2$. Doing the trigonometric manipulation we find that the probability that Bob gets a different answer to Alice (that is, Bob reads "0") given that Alice has transmitted $| + >_z$ is given by $1/2 - 1/4 \sin 2\theta$. Eve, measuring at an angle θ, clearly disturbs the statistics of the rejected data. Following through the probabilities in the table we find that the

probability, q, that Alice and Bob disagree on examination of the data for which they measure different alphabets is

$$q=\frac{1}{2}-\frac{1}{4}\sin 2\theta \qquad (2)$$

Suppose that Alice and Bob compare M bit of data for which they have measured different alphabets (we have previously called this the "rejected" data, based on the BB protocol - we shall, for convenience continue with this usage, where appropriate). They would expect $M/2$ bits, on average, to disagree (or equivalently to agree). The probability of obtaining k errors is given by the k^{th} term in the binomial expansion

$$P(k\ errors)=\frac{M!}{k!\,(M-k)!}q^k(1-q)^{M-k} \qquad (3)$$

Using the definition of q as equation (2) above and writing

$$\sigma^2=\frac{M}{4}\left(1-\frac{1}{4}\sin^2 2\theta\right) \qquad (4)$$

we can approximate the probability of obtaining k disagreements between Alice and Bob by the gaussian distribution

$$P(k\ errors)\approx\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-\frac{1}{2\sigma^2}\left(k-\frac{M}{4}[2-\sin 2\theta]\right)^2\right) \qquad (5)$$

This is a very good approximation for large M (it is reasonably good even for M as little as 10). The expected distribution occurs at $\theta = 0$ and we find that under the same approximation the expected probability distribution

for the number of disagreements or errors, labelled as $P_{EXP}(k \text{ errors})$ is given by

$$P_{EXP}(k\ errors) \approx \sqrt{\frac{2}{M\pi}} \exp\left(-\frac{2}{M}[k-M/2]^2\right) \tag{6}$$

For future notational convenience we shall denote the expected and actual probability distributions using the single argument k, that is the actual distribution becomes $P(k)$ and the expected $P_{EXP}(k)$. If Eve intrudes on the channel at some arbitrary angle (most likely to be $\theta = \pi/4$) then Alice and Bob will be able to detect this simply by counting the number of disagreements they obtain. For large M the expected and actual distributions are of the order of $\sqrt{M}$ standard deviations apart. Eve is likely to cause an abnormal number of disagreements, or agreements, which will be extremely unlikely to fall within the expected probability range. The degree of confidence can be set by Alice and Bob by setting some threshold at a specified number of standard deviations from their expected mean value (for example, for gaussian distributions about 98% of the results fall within 3 standard deviations of the mean).

In order to see how this works in practice we shall assume an attack in an intermediate basis by Eve. Alice and Bob decide to set their threshold at some number of errors k_{th}. The probability, $P(Eve < k_{th})$, that Eve causes fewer errors than this threshold value is given by

$$P(eve<K_{th}) = \int_0^{K_{th}} P(k)\,dk \approx \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} \exp(-w^2/2)\,dw \tag{7}$$

where we have written the upper limit λ as

$$\lambda = \frac{1}{\sigma}\left(k_{th} - \frac{M}{4}(2 - \sin 2\theta)\right)$$

(8)

The probability, $P_{EXP}(<k_{th})$, that fewer than k_{th} errors arise from the expected distribution is given by

$$P_{EXP}(k_{th}) = 1 - \int_0^{M-k_{th}} P_{EXP}(k)\,dk \approx 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda_{EXP}} \exp(-w^2/2)\,dw$$

(9)

where we have written the upper limit as

$$\lambda_{EXP} = (M - 2k_{th})/2\sigma$$

(10)

Eve actually causes the number of disagreements to fall by her intervention, hence the thresholding is set as above. At M = 24, a threshold set at k_{th} = 9 and an attack by Eve in the Breidbart basis we find that P ($Eve < k_{th}$) ≈ 0.9207 so that Eve is approximately 92% likely to trigger the "alarm" set by Alice and Bob. However, for this threshold, the expected distribution is approximately 11% likely to trigger the alarm. These statistics improve as M increases and change according to the level of confidence required. For example, in the above case with M = 24 the threshold can be set at k_{th} = 7.5 in which case we have $P(Eve < k_{th})$ ≈ 0.7612, but $P_{EXP}(< k_{th})$ ≈ 0.033 so that Eve is only about 76% likely to trigger the alarm. However, if the alarm is triggered then it is only about 3% likely to have been a result of the expected distribution. The threshold must be set as the users of the channel feel appropriate as M increases it becomes ever more difficult for Eve to intrude without triggering the alarm. Furthermore, any triggered

alarm is much less likely to have been an accident (subject to appropriate thresholding).

The above consideration of the rejected data can be used in conjunction with the BB protocol to generate a new modified protocol. This adapted protocol can now be described as follows:

1. Alice and Bob randomly choose between spin-x and spin-z alphabets.

2. Alice and Bob communicate, possibly over a public channel (e.g. telephone) to discuss their data. The consider the rejected data first and subject this to the statistical test described above. This determines whether Eve has attempted to eavesdrop in a different alphabet to that of Alice or Bob.

3. If this data is "eavesdropper-free", according to the level of confidence set by Alice and Bob, they now use part of the standard BB protocol to determine whether an eavesdropping attempt has been made in the alphabets used by Alice and Bob (the standard BB protocol can detect the presence of an eavesdropper using any alphabet, as described above. However, by consideration of the rejected data the eavesdropper cannot use an intermediate alphabet to any advantage).

We now describe a new protocol for which it is not necessary to compare any of the potentially useful key data and only requires comparison of rejected data:

1. Alice randomly selects between 3 alphabets; the spin-x, the spin-z and spin-$\pi/4$ alphabets.

2. Bob randomly chooses between spin-x and spin-z alphabets. Alice and Bob will use the same alphabets 1/3 of the time, on average.

3. Alice and Bob now select that data for which Alice used spin-x or spin-z and Bob measured in a different alphabet to that of Alice. This allows the statistical test for interception in an alphabet intermediate to the x or z alphabets. On average 1/3 of the data is used for this purpose.

4. If an eavesdropper has not been detected at this stage Alice and Bob now compare the results when Alice used spin-$\pi/4$ transmissions. Again this uses 1/3 of the data, on average. A statistical test, as described above, will now determine the presence of an eavesdropper who has used the spin-x and/or spin-z alphabets to attempt to intercept the key.

5. If no eavesdropper has been detected Bob and Alice can now assume, to within their pre-determined confidence level that no eavesdropping attempt has been made. The data for which Alice and Bob used the same alphabets should now be shared secret information and can be used as a key.

An alternative coding scheme offering greater symmetry uses spin-z, spin-$\pi/3$, and spin-$2\pi/3$ alphabets. In general this selection of alphabets is to be preferred as giving a greater deviation in the measured statistics in response to Eve's eavesdropping. Although the above example describes a scheme whereby Bob measures only two alphabets, Bob can in fact choose to measure in either two or all three of the transmitted alphabets. The analysis presented above can be trivially generalised to include this situation.

The standard BB protocol can also be used in conjunction with this new rejected data protocol to give an even greater degree of security.

Information-Theoretic Basis

Central to the generality of the technique is the demonstration that any eavesdropper unavoidably disturbs a quantum channel, irrespective of which dimensionality of alphabet is used. We shall assume that Alice and Bob are to communicate using two alphabets sourced by the operators $\hat{A}$ and $\hat{B}$ with eigenvalues $|\{\alpha_j\}>$ and $|\{\beta_k\}>$, respectively, and of dimensionality N. The channel transition probabilities, determined by the laws of quantum mechanics, in the absence of an eavesdropper, Eve, are given by the overlap integrals $|<\alpha_j|\beta_k>|^2$ which give the probability that Bob receives the symbol $|\beta_k>$ given that Alice transmitted the symbol $|\alpha_j>$. We shall further assume, for

convenience, that Alice makes an equal a priori choice of input symbols. The system mutual information, or the information flow rate between Alice and Bob, is, from standard information theory, given by

$$J(\hat{A},\hat{B}) = 1nN + \frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N} |\langle\alpha_j|\beta_k\rangle|^2 1n|\langle\alpha_j|\beta_k\rangle|^2 \qquad (11)$$

Clearly the channel capacity is $1nN$. If $\hat{A}$ and $\hat{B}$ are conjugate then $|\langle\alpha_j|\beta_k\rangle|^2 = 1/N$ (for $N = 2$, the spin-z and spin-x operators are conjugate), and we have that $J(\hat{A},\hat{B}) = 0$. For the $N = 2$ case this occurs when Alice uses spin-z and Bob uses spin-x, for example, and Bob therefore reads the symbols "1" or "0" with equal likelihood. There is no correlation, therefore, between input and output symbols and no information is transmitted between Alice and Bob in this case.

Let us now suppose that an eavesdropper tries to intrude using an alphabet sourced by an operator $\hat{E}$ consisting of the symbols $|\{\epsilon_m\}\rangle$. The channel transition probability between Alice and Bob is now given by

$$\Gamma_{jk} = \sum_{m=1}^{N} |\langle\alpha_j|\epsilon_m\rangle|^2 |\langle\epsilon_m|\beta_k\rangle|^2 \qquad (12)$$

The system mutual information flow rate is now given by

$$J_E(\hat{A},\hat{B}) = 1nN + \frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N} \Gamma_{jk} 1n\Gamma_{jk} \qquad (13)$$

where we have used the subscript E to denote the information flow rate in the presence of an eavesdropper. The crucial point to note is that, in general, $J(\hat{A},\hat{B}) \neq J_E(\hat{A},\hat{B})$ so that the presence of Eve changes the information flow rate on the channel. If we define the parameter ξ by

$$\xi = \frac{J_E(\hat{A},\hat{B}) - J(\hat{A},\hat{B})}{J^{max}(\hat{A},\hat{B})}$$

(14)

where J^{max} describes the maximum possible information flow between Alice and Bob given their initial choice of alphabets and symbols. In our case, by assumption, J^{max} is simply the channel capacity and is $\ln N$. This new parameter measures the degree of disturbance introduced by the eavesdropper and varies as

$$-1 \leq \xi \leq 1,$$

(15)

so that a negative value implies a reduction in the information flow rate between Alice and Bob (the regime exploited by the BB protocol). A positive value of ξ implies that the eavesdropper has caused an information flow (the regime exploited by the new protocols described above). If $\xi = 0$ then the presence of an eavesdropper cannot be detected. If $\xi \neq 0$ then an eavesdropper is always, in principle vulnerable to detection. The condition for $\xi = 0$, that is, the eavesdropper remains undetected, is equivalent to the choice $\Gamma_{jk} = |\langle\alpha_j|\beta_k\rangle|^2$. This can only be achieved if the eavesdropper chooses the operator $\hat{A}$ every time that Alice uses this operator and also chooses the operator $\hat{B}$ every time that Alice uses this operator. If Alice chooses randomly between $\hat{A}$ and $\hat{B}$ then Eve's chances of using the same operator as Alice every time, and therefore escaping detection, are negligible.

This analysis can clearly be generalised to situations where Eve's strategy involves measurement of more than one operator [8].

Alternative Implementations

The protocols we have developed are not limited in applicability to PON's of the type described above, but may be used with any communication channel that is accurately modelled by the formalism we have developed for quantum

alphabets. Thus we could envisage making use of single electrons as the carriers of information. Any communication for which the alphabet symbols are quantum states can be examined in the way described here and the quantum cryptographic protocols applied.

Also, alternative statistical tests may be used to detect the effect of Eve on the rejected data. For example, the effect on Bell's inequality may be examined. The violation of this inequality is characteristic of purely quantum channels, and the effect of Eve can be regarded as degrading the purely quantum nature of the channel between Alice and Bob, tending to restore the Bell inequality. If the encoding operators, which as above may correspond to operations on the phase or polarisation of photons, are represented by the scalar products of unit verctors a, b or c with a spin-1/2 operator σ and P (a,b) is the probability that Alice and Bob agree minus the probability that they disagree, then the Bell inequality may be expressed as

$$B = 1 - P(b, c) - |P(a, b) - P(a, c)| \geq 0.$$

If an eavesdropper is present on the channel she will tend to cause this inequality to be satisfied. If no eavesdropper is present, and Alice and Bob employ certain alphabets (preferably z, $\pi/3$ and $2\pi/3$ as these cause the maximal violation) then they will see a violation of this inequality and B becomes negative. Thus statistical tests can be used to set a threshold for the security in much the same way as described above.

REFERENCES

1. C.H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, in "Advances in Cryptology: Proceedings of Crypto '82", (Plenum, New York, 1983); C.H. Bennett and G. Brassard, IBM Technical Disclosure Bulletin, **28** 3153 (1985); C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, J. Cryptology, **5** 3 (1992).

2. S. Wiesner, SIGACT News, **15** 78 (1983)

3. A. K. Ekert, Phys. Rev. Lett., **67** 661 (1991)

4. C.H. Bennett, G. Brassard and N. D. Mermin, phys. Rev. Lett., **68** 557 (1992).

5. Phoenix SJD, Barnett SM, Journal of Modern Optics 1993, Vol 40. No. 8. 1443-1448.

6. S.M. Barnett and S.J.D. Phoenix, *Phys. Rev. A*, 48 R5 (1993).

7. K.J. Blow and S.J.D. Phoenix, *J. Mod. Opt.*, 40 33 (1993).

8. S.M. Barnett, B. Huttner and S.J.D. Phoenix, *J. Mod. Opt.*, in press.

CLAIMS

1. A method of operating a communication system using single-channel quantum cryptography characterised by the steps of analysing rejected data determined to have been transmitted and received using different operators at the transmitter and receiver and comparing the expected and measured relationship between the data transmitted and received to detect whether an eavesdropper is present.

2. A method according to claim 1, including the steps of both comparing the statistics of the transmitted and received rejected data to determine whether any eavesdropper has detected the communicated signal using a different quantum alphabet to those used by the transmitter and receiver; and

subsequently testing at least a sample of the other data to determine whether any eavesdropper has detected the communicated signal using a coding alphabet used by the transmitter and receiver.

3. A method according to claim 1, in which testing to detect an eavesdropper is carried out using rejected data only.

4. A method according to claim 1, 2 or 3, in which one of the transmitter and receiver encodes or decodes data using a selected one of three or more different coding alphabets, the three or more coding alphabets having symbols which are eigenstates of mutually non-commuting operators, and the other of the transmitter and receiver detects signals using at least two of the alphabets.

5. A method according to claim 4, in which the said one of the transmitter and receiver encodes or decodes the signals using one of spin-x, spin-z and spin-$\pi/4$ alphabets and the said other of the transmitter and receiver decodes the signal using at least two of those alphabets.

6. A method according to claim 4, in which the said one of the transmitter and receiver encodes the signal using one of spin-z, spin-$\pi/2$ and spin-$2\pi/3$ alphabets, and the

said other of the receiver and transmitter decodes the signal using at least two of these alphabets.

7. A method according to claim 5 or 6, in which separate tests are carried out on rejected data encoded with the orthogonal alphabets and on rejected data encoded with an intermediate alphabet.

8. A communication system comprising a single-photon source and a single-photon detector arranged to be connected to a communications channel, means for encoding a single photon signal from the single photon source using non-commuting quantum mechanical operators, means for detecting using non-commuting quantum mechanical operators a single photon signal received over the communications channel, and processing means for comparing the states of single photon signals as encoded and detected, thereby detecting the presence of any eavesdropper,

characterised in that the processing means include means for analysing data determined to have been encoded and decoded using different operators and comparing the expected and measured relationship between the data encoded and detected to detect any eavesdropper.

9. A system according to Claim 8, in which one of the means for encoding and the means for detecting is arranged to encode or decode respectively single photon signals using spin-z, spin-$\pi/2$ and spin-$2\pi/3$ operators, and the other of the means for encoding and the means for decoding is arranged to encode or decode using at least two of the three operators.

10. A system according to Claim 9, in which both the means for encoding and the means for decoding are arranged to encode and decode signals using selected ones of all three operators.

Fig.1.

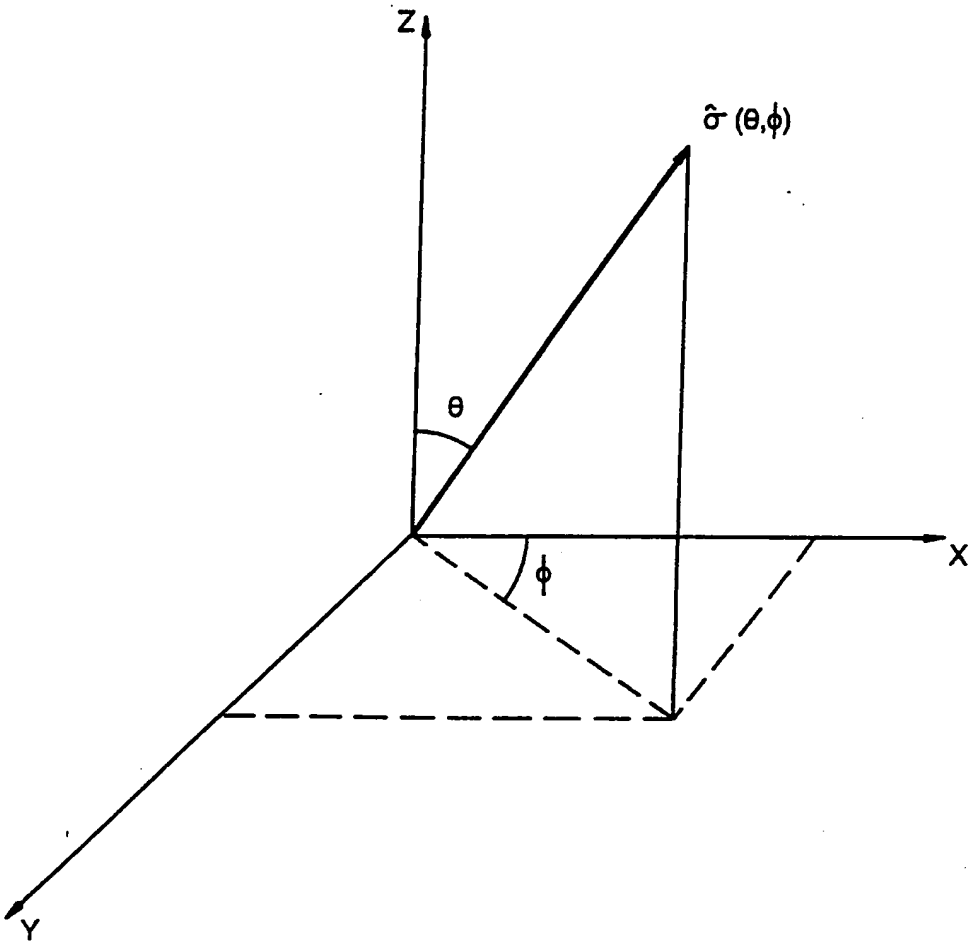
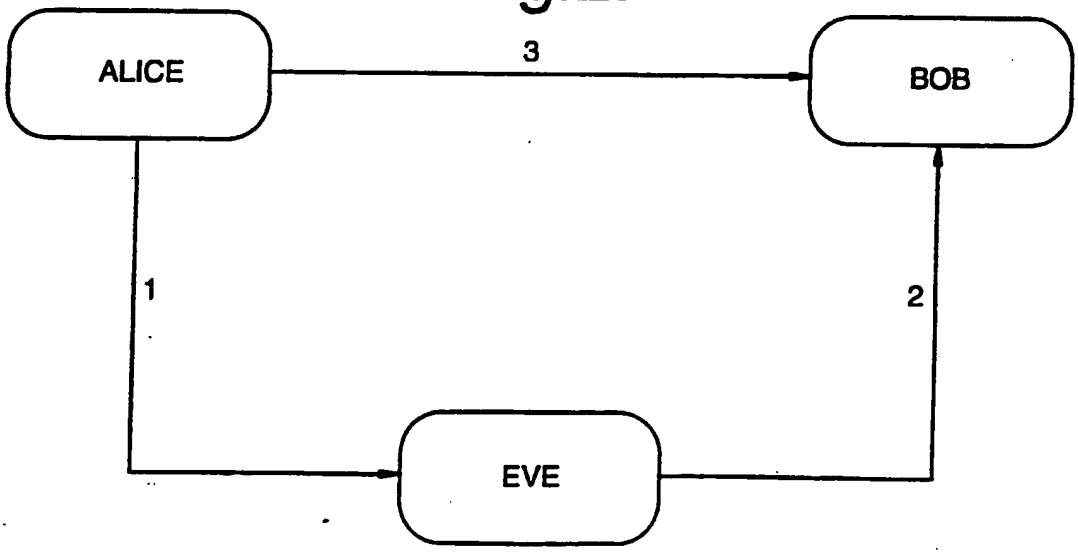


Fig.2.



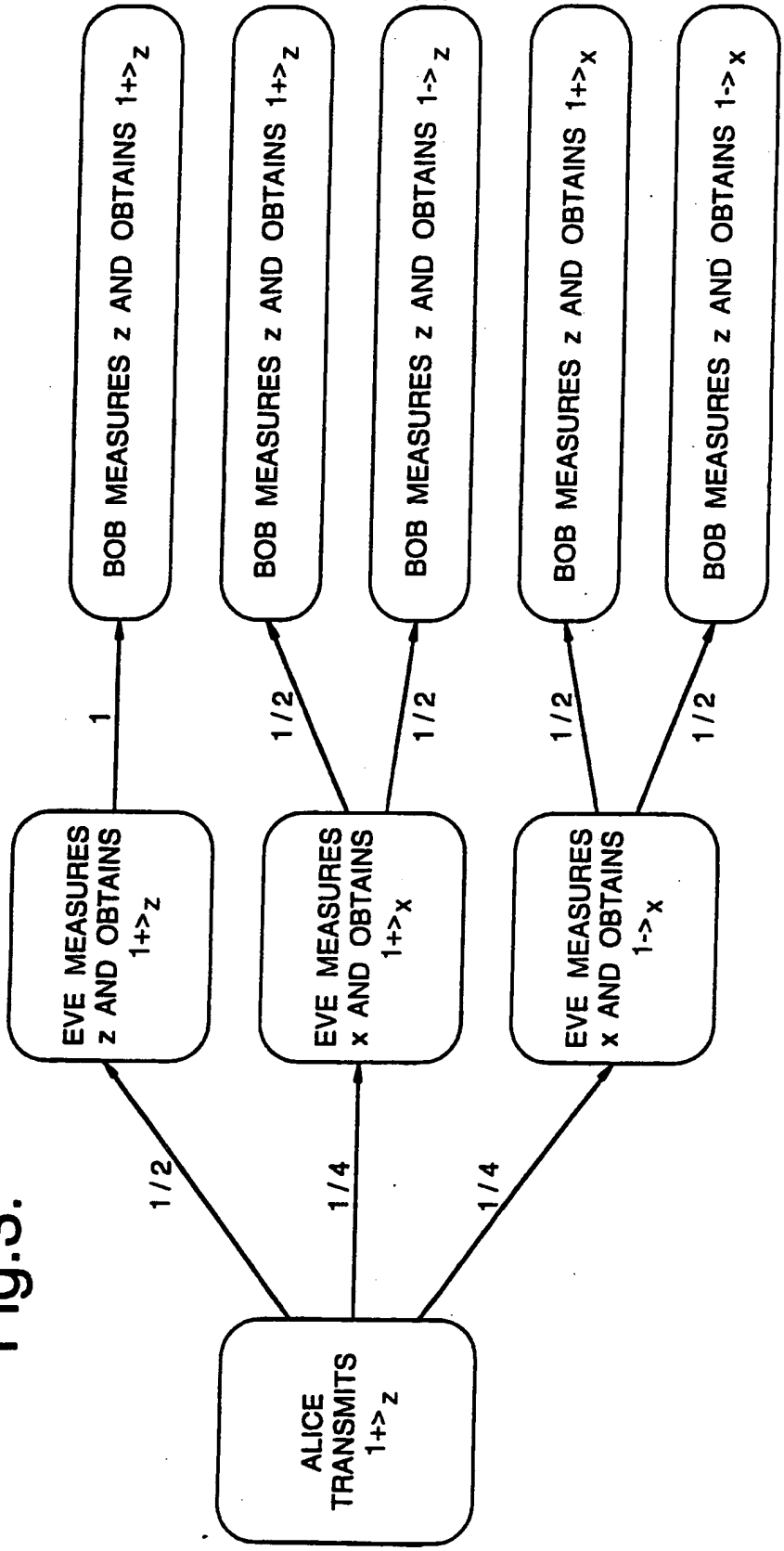

ALICE TRANSMITS 1+>z
1/2
1/4
1/4
EVE MEASURES z AND OBTAINS 1+>z
EVE MEASURES x AND OBTAINS 1+>x
EVE MEASURES x AND OBTAINS 1->x
1
1/2
1/2
1/2
1/2
BOB MEASURES z AND OBTAINS 1+>z
BOB MEASURES z AND OBTAINS 1+>z
BOB MEASURES z AND OBTAINS 1->z
BOB MEASURES z AND OBTAINS 1+>x
BOB MEASURES z AND OBTAINS 1->x

Fig.3.

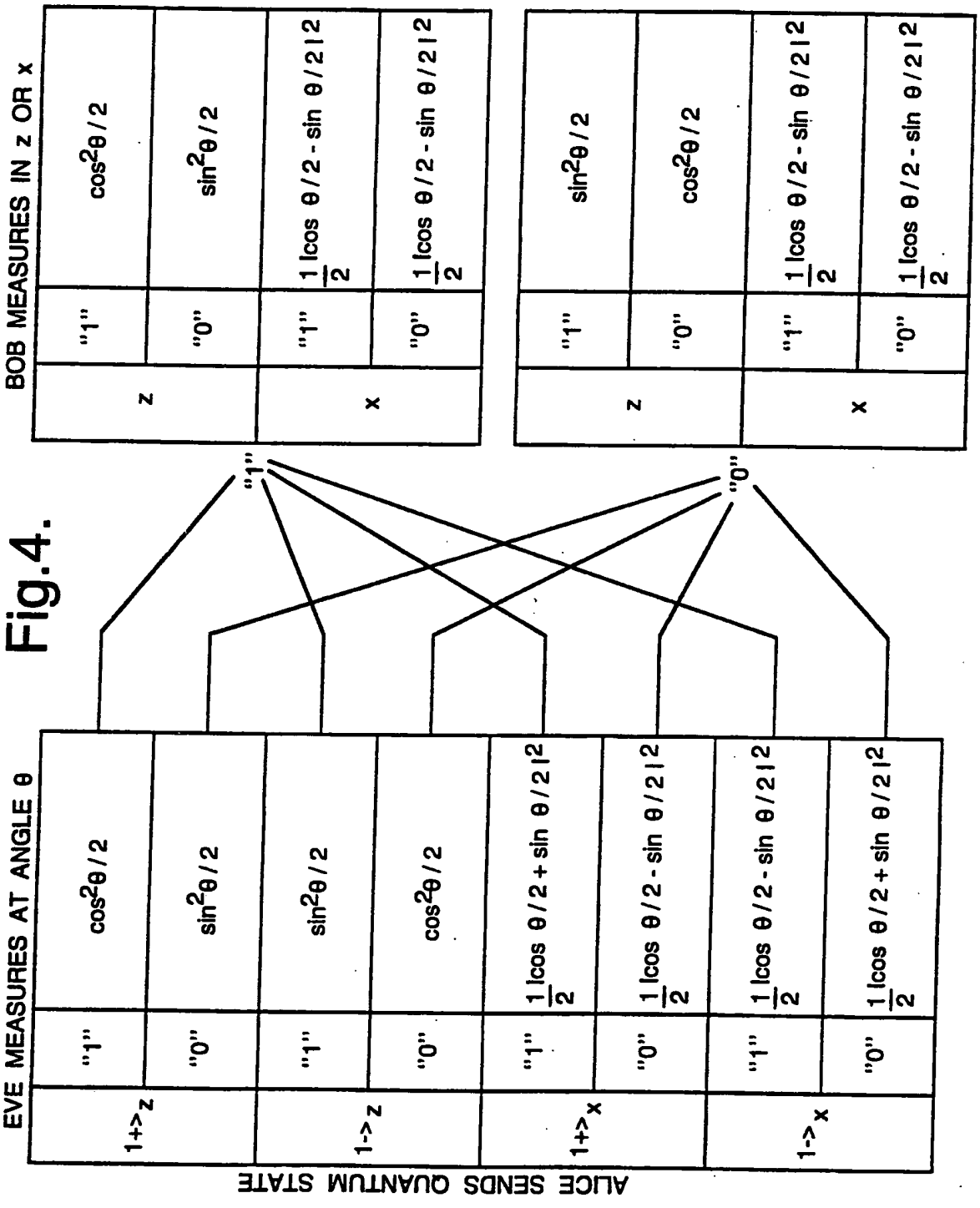

ALICE SENDS QUANTUM STATE
EVE MEASURES AT ANGLE θ
1+>z
1->z
1+>x
1->x
"1"
"0"
cos²θ/2
sin²θ/2
1/2 |cos θ/2 + sin θ/2|²
1/2 |cos θ/2 - sin θ/2|²
BOB MEASURES IN z OR x
z
x

Fig.4.

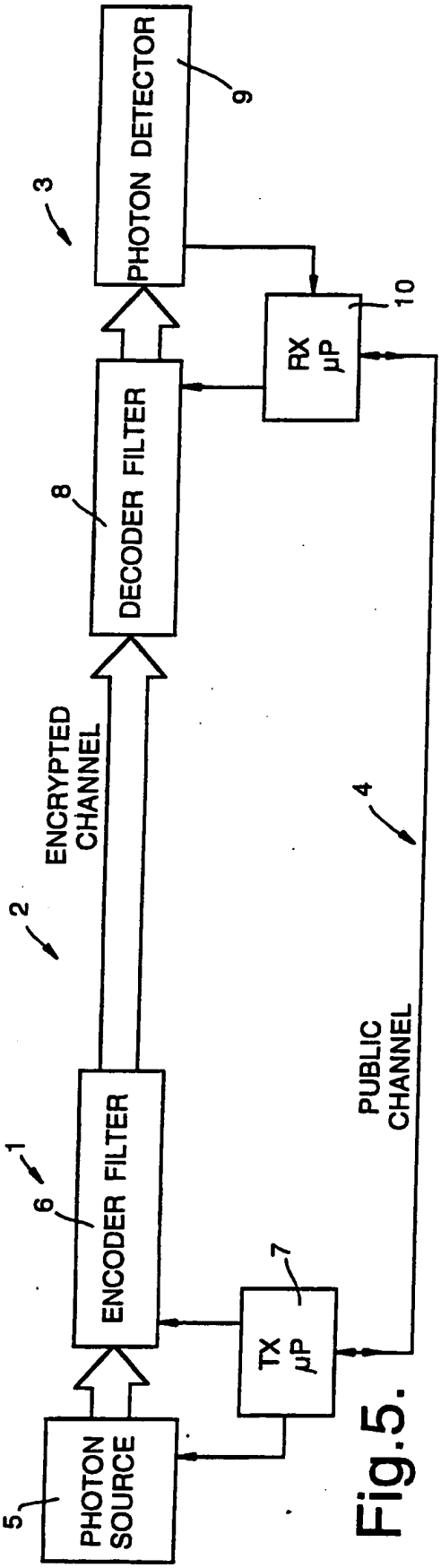

PHOTON DETECTOR
9
3
RX μP
10
DECODER FILTER
8
ENCRYPTED CHANNEL
2
PUBLIC CHANNEL
4
ENCODER FILTER
6
1
TX μP
7
PHOTON SOURCE
5

Fig.5.

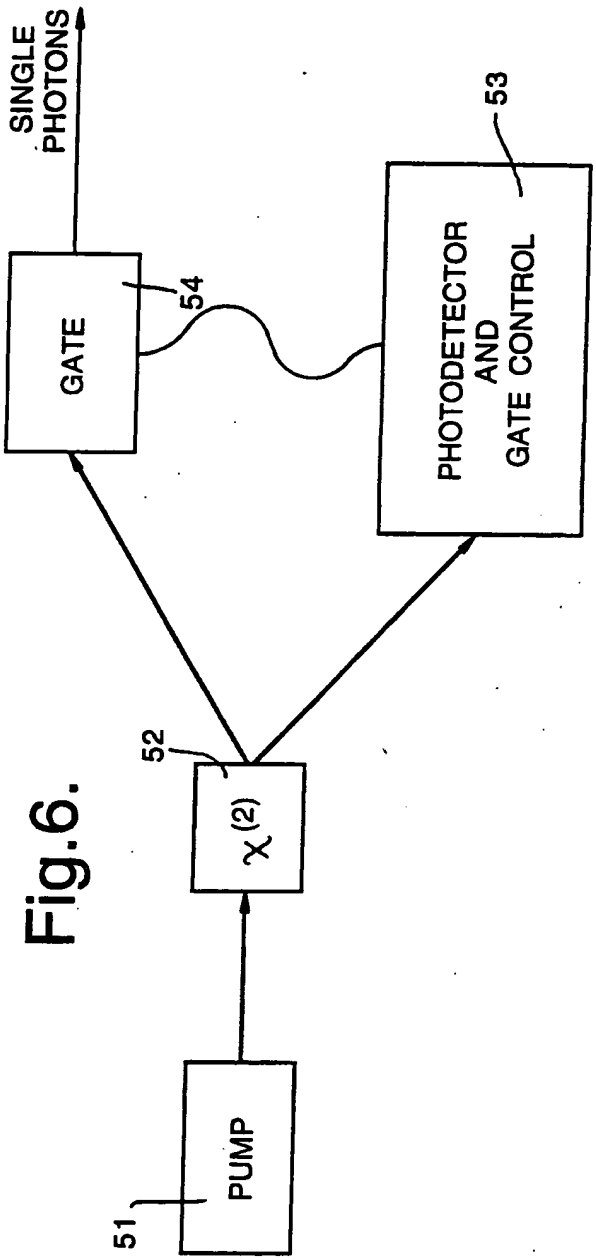

SINGLE PHOTONS
GATE
54
PHOTODETECTOR AND GATE CONTROL
53
52
$\chi^{(2)}$
PUMP
51

Fig.6.

Fig.7.

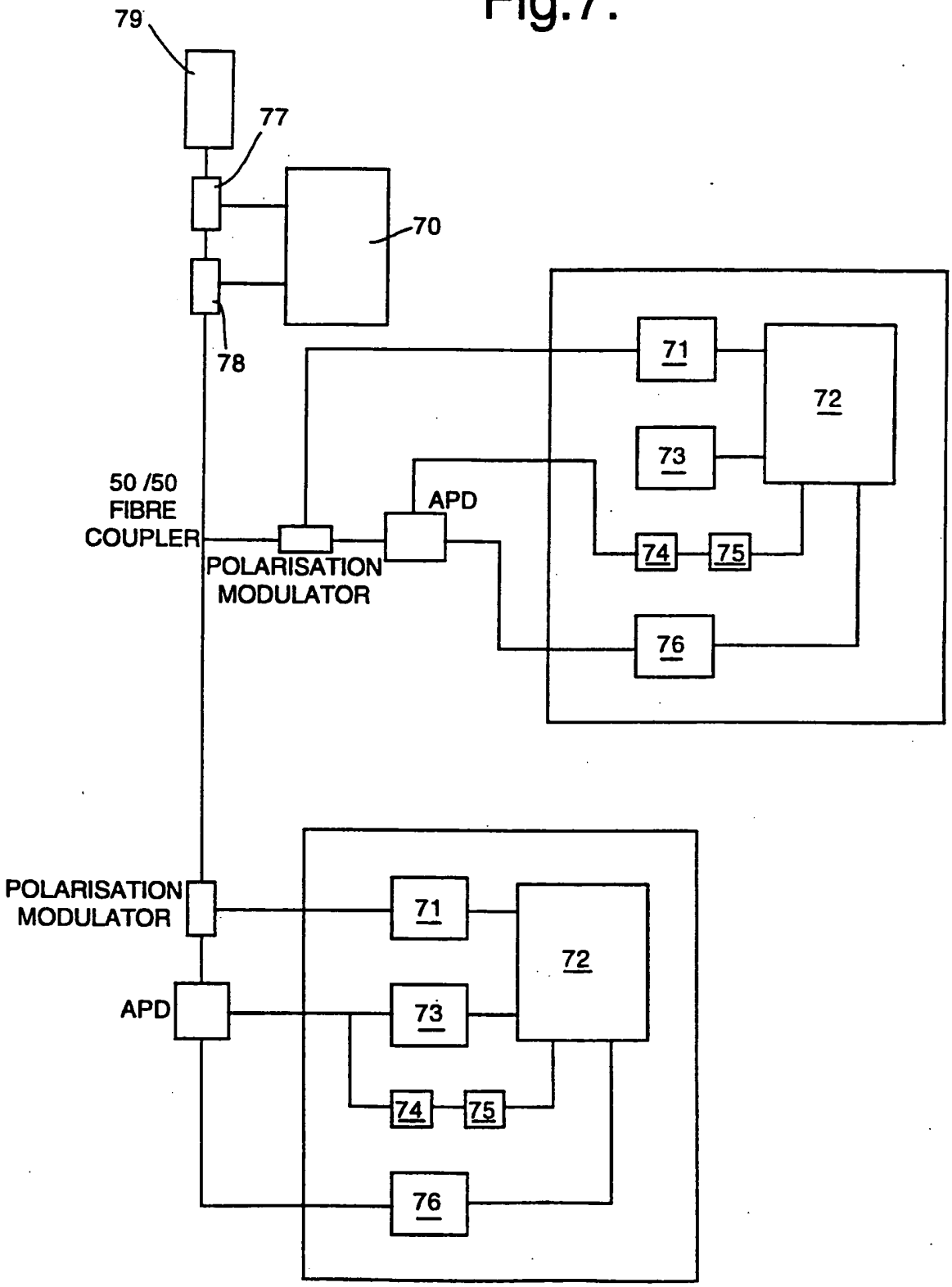

79
77
70
78
71
72
73
74
75
76
50 /50
FIBRE
COUPLER
APD
POLARISATION
MODULATOR
POLARISATION
MODULATOR
APD
71
72
73
74
75
76

Fig.8a.

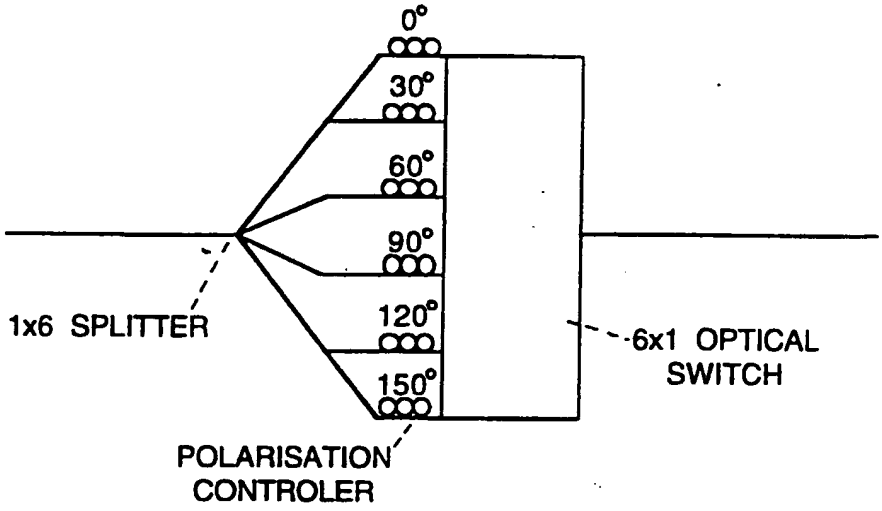
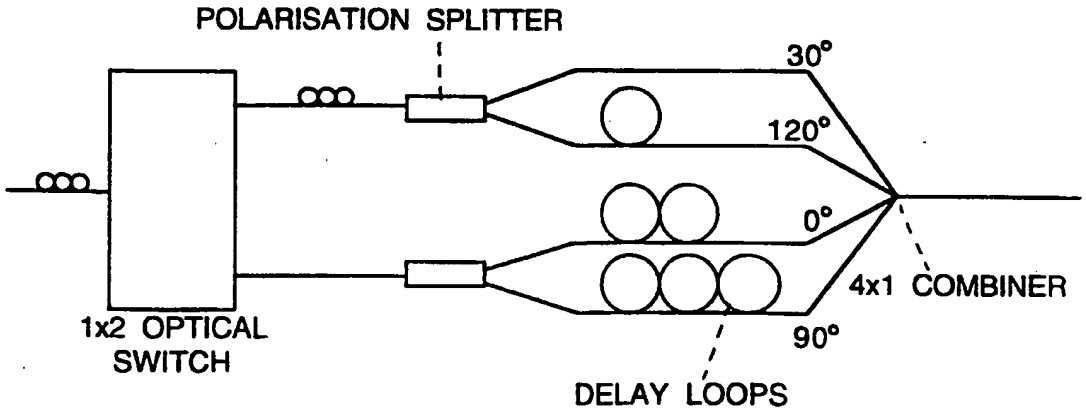

0°
30°
60°
90°
120°
150°
1x6 SPLITTER
6x1 OPTICAL SWITCH
POLARISATION CONTROLER

Fig.8b.


POLARISATION SPLITTER
30°
120°
0°
90°
4x1 COMBINER
1x2 OPTICAL SWITCH
DELAY LOOPS

INTERNATIONAL SEARCH REPORT

Inten nal Application No
PCT/GB 93/02075

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IBM TECHNICAL DISCLOSURE BULLETIN. vol. 28, no. 7 , December 1985 , NEW YORK US pages 3153 - 3163 'QUANTUM PUBLIC KEY DISTRIBUTION SYSTEM' cited in the application see page 3154, last paragraph see page 3155, paragraph 3 see page 3156, line 1 - page 3157, paragraph 2	1,4

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
16 December 1993	20.01.94
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Authorized officer Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)